International Journal of Trendy Research in Engineering and Technology
Volume 4 Issue 2 April 2020
ISSN NO 2582-0958
IJTRET

A DISTRIBUTED MACHINE LEARNING BASED IDS FOR CLOUD COMPUTING

B.Bhagavathy Preetha[1], A.B.Harsha Vardhni[1], M.Monica[1]

Dr.R.Geetha[2]

UG Students[1], Professor[2] ,Department of Computer Science and Engineering
S.A.Engineering College, Chennai – 77.
1616003@saec.ac.in[a)], 1616010@saec.ac.in[b)], 1616023@saec.ac.in[c)]

ABSTRACT

Typically an IDS refers to a software application that monitors a network for intrusion or malicious activity. It signals an alarm once an intrusion is detected. In this paper, an IDS based on Distributed Machine Learning that detects phishing attacks and issues an alarm when the intrusion is detected has been discussed. This is done by using SVM as the base algorithm. More on why SVM is used and how the IDS can be applied to detect other types of intrusion has been discussed.

I. INTRODUCTION

Information which is existing in servers can be accessed by hackers through web server attacks. This can be achieved by hacking into servers through the URLs of servers. The users will be hacked when they browse or download documents from web servers which has been injected with malicious code.

Detecting these web attacks using Traditional IDS such as snort and web application firewalls (WAF) has been proved to be penetrable. Hence applying deep learning techniques to detect these web attacks is difficult since different attacks possess different signatures depending upon their URLs. A Distributed system for detecting web attacks from URLs has been proposed through deep learning like CNN and other models which utilize NLP.

A generic web attack detection system has been proposed which can enhance the stability through concurrent models. Phishing attack exploits poor handling of untrusted data. It could involve an attachment to an email that loads malware onto the computer. It could also be a link to an illegitimate website that can trick the user into downloading the malware or handling over our personal information.

A proxy is typically placed in front of the server to examine the server's responses before they reach a user's browser. Since a firewall uses a set of rules to permit or deny network connections, the intrusion will be prevented by assuming whether a set of rules have been detected or not. Thus, an IDS differs from traditional firewalls.

II. EXISTING SYSTEM

Emerging social network sites have made it easy to be attacked by cyber criminals every day. Social network sites where the users personal data maybe vandalized and untrusted data is handled poorly, phishing attacks are one that scams users by exploiting them to get hold of their bank accounts and passwords.

Blogs, forums, paste and doc sites are all part of the social media ecosystem[1]. The phishing attack may be either via Data Gathering, Impersonation, credential theft. Phishing attacks in social network sites can be presented only if the user is careful enough by not clicking on unfamiliar links and always checking whether that website is a legitimated website or not. By using some Antivirus or Anti-phishing software these attacks can be prevented.

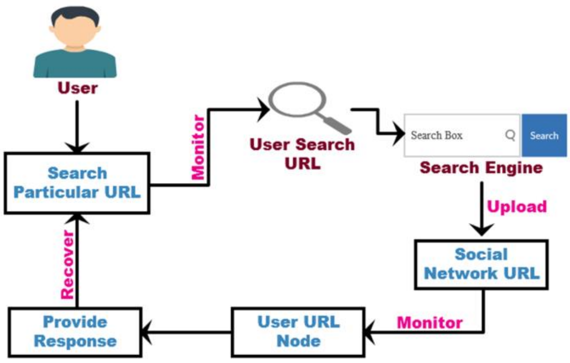
III. PROPOSED SYTEM

Search engines supply a highly effective means of information retrieving way. But the search engine is also a platform for spreading information. Because of these features, the propagators of malicious code have kept in step with search engines, building a hidden relationship within them. In recent years, so-called worms have utilized the search engine to spread themselves across the Web. A search engine is a quick and easy vehicle for malicious code to locate new targets. An IDS which can detect phishing attacks in a normal social network site without the use of Anti-phishing software has been proposed. If by accident, the user clicks on phishing malvertisements or links that leads to a phishing sites, a warning will be issued regarding the accessibility of the site and whether it is a legitimate website or not.

The phishing URL is detected based on SVM. SVM refers to Support Vector Machine. On using SVM classification, a warning message regarding the reliability of the website is based on the MATLAB based computer program. This is done to avoid users from becoming victims by losing their information.

IV. ARCHITECTURE DIAGRAM

The Architecture of the system is as follows:



The Modules involved in the Architecture Diagram are as follows:

1. Social Networks Module
2. Epidemic Module in Social Networks
3. Propagation Canalization Module
4. Feedback Module

Social networks module

With the proliferation of social networks and their ever increasing use, viruses have become much more prevalent. In this module the user login to the application and use search engine to search any content of data in the application to get the required data with respective to the keywords entered in the search engine.

Epidemic module in social networks

The user click the unofficial links and get access the data along with virus which get affected along with the retrieval of data then application. In a static network, weakly connected heterogeneous communities can have significantly different infection levels.

Propagation canalization module

Results show the significant influence of a search engine particularly its ability to accelerate virus propagation in social networks. In contrast, adaptation promotes similar infection levels and alters the network structure so that communities have more similar average degrees

Feedback module

Based on the user review, the acceleration of the virus in the official link has been predicted. Whenever the user visits any uniform resource locator (URL) through search engine. They will be redirected to the uniform resource locator (URL), the user will get the broader details about the link how much it affected or how much it is safe to access.

V. RELATED WORKS

An Algorithm to quantify the suspiciousness ratings of web pages based on similarity of visual appearance between web pages is proposed in this paper [2]. It is based on a rating method on weighted page-component similarity. In this paper [3], NFV is proposed to address capital and operational expense issues by implementing network functions as a pure software on commodity and general hardware. It has emerged as an approach to decouple the software networking processing and applications from their supported hardware and allow network services to be implemented as a software. Here [4], phishing websites are detected using Google's PageRank. Google gives a PageRank value to each site in the web. This work uses the PageRank value and other features to classify phishing sites from normal sites. Technologies of virtualization in a fog network[5], an anti-phishing gateway can be implemented as software at robust machine learning techniques for phishing detection. URL features and traffic features to detect phishing websites based on a designed neuro-fuzzy framework. A Heterogeneous classifier, to determine the phishing category through an intelligent anti-phishing strategy model for categorization of websites has been proposed [6].

VI. CONCLUSION

Thus an IDS, which focuses on phishing attacks has been proposed which issues an alarm when the link corresponding to phishing sites has been accessed by the user. This prevents the victim from losing untrusted data.

REFERENCES

[1] https://info.phishlabs.com/blog/how-social-media-is-abused-for-phishing-attacks

[2] Phishing-Alarm: Robust and Efficient phishing detection via Page component similarity, *Jian Mao, Wenqian Tian, Pei Li, Tao Wei and Zhenkai Liang,* "Volume 5, August 23, 2017, Digital Object Identifier 10.1109/ACCESS 2017.2743528"

[3]Software-defined Network function Virtualization: A Survey, *Yong Li, Min Chen,* "Volume 3, December 9, 2015, Digital Object Identifier 10.1109/ACCESS 2015.2499271"

[4]A PageRank based Detection technique for phishing Web sites,*A.Naga Venkata Sunil, Anjali Sardana,* "2012 IEEE Symposium on Computers & Informatics"

[5]Phishing-Aware: A Neuro Fuzzy approach for Anti-phishing on Fog networks,*Chuan Pham, Luong A.T.Nguyen, Nguyen H.Tran , Eui-Nam Huh, Choong Seon Hong,* "IEEE Transactions on Network and Service Management, DOI 10.1109/TNSM.2018.2831197"

[6] An Intelligent anti-phishing strategy model for Phishing Website Detection, *"Weiwei Zhuang, Qingshan Jiang, Tengke Xiong,* "2012, 32nd International Conference on Distributed Computing Systems Workshops, DOI 10.1109/ICDCSW.2012.66"